CLAIMS

What is claimed is:

1. A method comprising:

forming a request by a client to access encrypted content, wherein:

the request includes a persistent license for communication to a licensing server; and

the persistent license includes a key that is encrypted such that the key is not accessible by the client; and

receiving a license in response to the request, wherein the received license includes the key that is:

accessible by the client; and

for accessing the encrypted content.

2. A method as described in claim 1, further comprising:

forming an initial request for:

communication to the licensing server; and

storing encrypted content by the client;

receiving the persistent license at the client in response to the initial request; and

storing the encrypted content and the persistent license by the client.

3. A method as described in claim 1, further comprising:

forming an initial request by another client for:

communication to the licensing server; and

storing encrypted content by the other client;

receiving the persistent license at the other client in response to the initial request;

storing the encrypted content and the persistent license by the other client; and

obtaining the persistent license by the client from the other client.

4. A method as described in claim 1, wherein the received license is a boundary license and the key is a boundary key, and further comprising:

decrypting a session license utilizing a client key to obtain a session key;

decrypting the boundary license utilizing the session key to obtain the boundary key;

decrypting a content license utilizing the boundary key to obtain a content key; and

decrypting the encrypted content utilizing the content key.

5. A method as described in claim 4, wherein:

the session license includes access rules for the client for a session initiated between the client and the licensing server;

the boundary license includes access rules for the client for the encrypted content that is within a rights boundary in the encrypted content; and

the content license includes access rules for the client for the encrypted content.

6. A method as described in claim 4, wherein:

the persistent license was encrypted using an asymmetric encryption algorithm;

and

the encrypted content, the boundary license, and the content license were encrypted using respective symmetric encryption algorithms.

7. A method as described in claim 1, further comprising:

decrypting a session license utilizing a client key to obtain a session key, wherein the session license includes access rules for a session initiated between the client and the licensing server;

decrypting the received license utilizing the session key to obtain a decrypted boundary license, wherein:

the received license is an encrypted boundary license and the key within the boundary license is a boundary key; and

the boundary license includes access rules for content within a rights boundary in the encrypted content that is at least one of a television program and a television channel;

decrypting a content license utilizing the boundary key to obtain a content key, wherein the content license includes access rules for the encrypted content; and

decrypting the encrypted content utilizing the content key, wherein the encrypted content includes at least a portion of a television broadcast.

8. A method as described in claim 1, wherein the key is for decrypting the encrypted content.

9. A method as described in claim 1, wherein the encrypted content is streamed to the client.

10. One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 1.

11. A method comprising:

forming a request by a client for communication to a licensing server, wherein the request is for storing encrypted content by the client;

receiving a persistent license at the client in response to the request, wherein:

the persistent license includes a key that is encrypted;

the key, when decrypted, provides access to the encrypted content;

the key is configured to be decrypted by the licensing server; and

the client is not configured to decrypt the key from the persistent license; and

storing the persistent license and the encrypted content by the client.

12. A method as described in claim 11, further comprising:

forming a subsequent request by the client to access the stored content, wherein the subsequent request:

is for communication to the licensing server; and

includes the persistent license; and

receiving a second license at the client in response to the subsequent request,

wherein:

the second license includes the key; and

the second license is configured to be decrypted by the client such that the client obtains access to the key.

13. A method as described in claim 11, further comprising:

forming a subsequent request by another client to access the stored content, wherein the subsequent request:

is for communication to the licensing server; and

includes the persistent license; and

receiving a second license at the other client in response to the subsequent request, wherein:

the second license includes the key; and

the second license is configured to be decrypted by the other client such that the other client obtains access to the key.

14. A method as described in claim 11, wherein the encrypted content is streamed to the client.

15. A method as described in claim 11, wherein the license includes a certificate for verifying the licensing server by the client.

16. One or more computer-readable media comprising computer-executable

instructions that, when executed, perform the method as recited in claim 11.

17. A method comprising:

forming a first request for communication to a licensing server, wherein the first request is for storing encrypted content;

receiving a persistent license in response to the request, wherein the persistent license includes a boundary key;

storing the persistent license and the content;

forming a second request to access the encrypted content, wherein the second request includes the persistent license;

sending the second request to the licensing server;

receiving a boundary license in response to the second request, wherein the boundary license includes the boundary key;

decrypting the boundary license using a session key to obtain the boundary key;

decrypting a content license using the boundary key to obtain a content key; and

decrypting the encrypted content using the content key.

18. A method as described in claim 17, wherein the forming of:

the first request is performed by a first client; and

the second request is performed by a second client.

19. A method as described in claim 17, wherein the first and second requests are formed by a client.

20. A method as described in claim 17, further comprising at least one of decoding the decrypted content and outputting the decoded content.

21. A method as described in claim 17, wherein:

the persistent license was encrypted using an asymmetric encryption algorithm; and

the content, the boundary license, and the content license were encrypted using respective symmetric encryption algorithms.

22. One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 17.

23. A client comprising:

a processor; and

memory configured to maintain:

a persistent license including a key that is encrypted; and

a playback application that is executable on the processor to:

form a request to access encrypted content, wherein the request:

is for communication to a licensing server; and

includes the persistent license;

receive a response to the request that includes the key; and

access the encrypted content utilizing the key.

24. A client as described in claim 23, wherein the key is for decrypting the encrypted content.

25. A client as described in claim 23, wherein:

the memory is further configured to maintain a content license;

the key included in the persistent license is for decrypting the content license;

the content license includes a content key; and

the content key is for decrypting the encrypted content.

26. A client as described in claim 23, wherein:

the memory is further configured to maintain a content license;

the key included in the persistent license is for decrypting the content license;

the content license includes a content key;

the content key is for decrypting the encrypted content; and

the playback application is executable to:

decrypt the content license using the key to obtain the content key; and

decrypt the content using the content key.

27. A client as described in claim 23, wherein:

the memory is further configured to maintain a session license, a content license, and a client key;

the client key is for decrypting the session license;

the session license includes a session key for decrypting the response;

the response is a boundary license;

the key included in the response is a boundary key for decrypting the content license;

the content license includes a content key; and

the content key is for decrypting the encrypted content.

28. A client as described in claim 23, wherein:

the memory is further configured to maintain a session license, a content license, and a client key;

the client key is for decrypting the session license;

the session license includes a session key for decrypting the response;

the response is a boundary license;

the key included in the response is a boundary key for decrypting the content license;

the content license includes a content key;

the content key is for decrypting the encrypted content; and

the playback application is executable to:

decrypt the session license using the client key to obtain the session key;

decrypt the boundary license using the session key to obtain the boundary key;

decrypt the content license using the boundary key to obtain the content key; and

decrypt the content using the content key.

29. A client as described in claim 23, wherein the playback application is further executable to:

form an initial request for:

communication to the licensing server; and

storing encrypted content by the playback application;

receive the persistent license in response to the initial request; and

store the encrypted content and the persistent license.

30. A client as described in claim 23, wherein the playback application is further executable to form a request to obtain the encrypted content from another client.

31. A client as described in claim 23, further comprising a tuner configured to receive the encrypted content when streamed over a network.

32. A client as described in claim 23, wherein the license includes a certificate for verifying the licensing server.

33. A system comprising:

a network;

a client including:

a persistent license having a key that is encrypted; and

a playback application that is executable to:

form a request to access encrypted content, wherein the request includes the persistent license;

receive a response to the request that includes the key; and

access the encrypted content utilizing the key; and

a licensing server including a licensing module that is executable to:

receive the request including the persistent license;

decrypt the persistent license to obtain the key; and

form the response that includes the key for communication to the client over the network.

34. A system as described in claim 33, wherein:

the client includes a content license;

the key included in the persistent license is for decrypting the content license;

the content license includes a content key; and

the content key is for decrypting the encrypted content.

35. A system as described in claim 33, wherein:

the client includes a content license;

the key included in the persistent license is for decrypting the content license;

the content license includes a content key;

the content key is for decrypting the encrypted content; and

the playback application is executable to:

decrypt the content license utilizing the key to obtain the content key; and

decrypt the content utilizing the content key.

36. A system as described in claim 33, wherein:

the client includes a session license, a content license, and a client key;

the client key is for decrypting the session license;

the session license includes a session key for decrypting the response;

the response is a boundary license;

the key included in the response is a boundary key for decrypting the content license;

the content license includes a content key; and

the content key is for decrypting the encrypted content.

37. A system as described in claim 33, wherein:

the client includes a session license, a content license, and a client key;

the client key is for decrypting the session license;

the session license includes a session key for decrypting the response;

the response is a boundary license;

the key included in the response is a boundary key for decrypting the content license;

the content license includes a content key;

the content key is for decrypting the encrypted content; and

the playback application is executable to:

decrypt the session license utilizing the client key to obtain the boundary key;

decrypt the boundary license utilizing the session key to obtain the boundary key;

decrypt the content license utilizing the boundary key to obtain the content key;

decrypt the content utilizing the content key; and

play the decrypted content.

38. A system as described in claim 33, wherein the key is for decrypting the encrypted content.

39. A system as described in claim 33, wherein the persistent license is encrypted with an asymmetric encryption algorithm and the server includes a server private key for decrypting the persistent license.

40. A system as described in claim 33, wherein the playback application is further executable to:

form an initial request for:

communication to the licensing server; and

storing encrypted content by the playback application;

receive the persistent license in response to the initial request; and

store the encrypted content and the persistent license.

41. A system as described in claim 33, wherein the playback application is further executable to form a request to obtain the encrypted content from another client.

42. A system as described in claim 33, wherein the encrypted content is streamed to the client over the network.